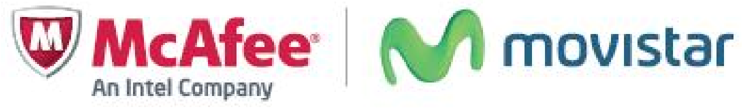
# Manual de Usuario de PC Seguro






## ÍNDICE







# 1. Introducción

Telefónica de España pone a su disposición ***PC Seguro*, **un producto que instalado en los equipos de su empresa le permite una gestión global de los mismos.

La funcionalidad **Antivirus** del servicio ***PC Seguro*** comprueba automáticamente la presencia de virus y malware y los elimina.

La funcionalidad **Firewall** ofrece una protección avanzada para los ordenadores de su empresa y sus datos confidenciales estableciendo una barrera entre los ordenadores e Internet y controlando el tráfico por Internet en busca de incidentes sospechosos.

La funcionalidad

Cuando Usted contrata **PC Seguro** está adquiriendo una licencia de uso y disfrute de que protege los equipos de su empresa.

# 2. Características

Una vez terminada la instalación inicial en los equipos correspondientes, se ejecuta de forma invisible en el PC, se actualiza automáticamente con los archivos de definición de virus (DAT) más recientes. A continuación envía informes al servidor que describen el estado actual de todos los ordenadores de la empresa con información sobre infecciones o brotes advertidos.

Proporciona protección constante frente a virus desde todas las localizaciones posibles. El servicio se pone en marcha al arrancar el ordenador y se mantiene activo hasta que se apaga.

El módulo ***Antivirus*** ofrece:

- **Protección continua:** vigila en silencio todas las entradas y salidas de archivos, las descargas, las ejecuciones de programas y demás actividades relacionadas con el sistema.
- **Descubrimiento instantáneo:** cuando detecta un virus, trata de desinfectar o eliminar el archivo infectado antes de que se produzcan más daños.
- **Actualización automática:** vigila continuamente el sistema y compara los archivos de definición de virus (DAT) con la versión más reciente. Cuando detecta un DAT nuevo, lo obtiene automáticamente.
- **Sistema de advertencia precoz AVERT:** utiliza la información de amenazas y brotes de virus más reciente descubierta por los laboratorios AVERT, una división de McAfee, nuestro proveedor de software para este producto.

Las principales características y funciones son:
Cada vez que se accede a un archivo del ordenador, lo explora para comprobar que no tiene virus u otras amenazas. Si detecta alguno, lo elimina o pone en cuarentena, guarda la información y la transmite al servidor para elaborar informes.

El módulo **Firewall** presenta las siguientes características:

- Protege frente a posibles exploraciones y ataques de *hackers*
- Complementa las defensas antivirus





- Supervisa Internet y los incidentes de la red
- Alerta de incidentes potencialmente hostiles
- Ofrece información pormenorizada sobre el tráfico sospechoso por Internet

Funcionalidades de ***Firewall***:

- **Manejo inteligente de aplicaciones**
  Cuando una aplicación busca acceso a Internet, *Firewall* comprueba primero si la aplicación se reconoce como segura o dañina. Si se reconoce como segura, Firewall le autoriza automáticamente el acceso a Internet para que no tenga que hacerlo el usuario.

- **Función de alerta mejorada**
  Para poder trabajar con estas nuevas funciones, se ha actualizado la interfaz de usuario y su mecanismo de alerta. Consulte el apartado “Acerca de las alertas” para ver información detallada sobre los tipos de alertas que pueden aparecer y las posibles respuestas que puede elegir.

La actualización regular de los módulos de la protección es la base del servicio. En una situación simple, cada estación de trabajo se conecta directamente al Centro de Operaciones de Red (NOC) a través de Internet y comprueba si hay actualizaciones nuevas de los archivos de definición de virus (DAT), del motor de exploración o de la versión del producto. Varias funciones ayudan a utilizar de forma eficaz los recursos de red; por ejemplo:

El módulo ***Filtrado de contenido Web*** ofrece:

- **Protección del navegador:** notifica al usuario cuando acceda a sitios Web que puedan contener contenido de riesgo (por ejemplo phising) a través de una notificación en su navegador (verde, ambar o rojo) en función de su reputación.
- **Filtrado de contenido:** permite filtrar el acceso a sitios web cuyo contenido no se considere adecuado en función de su clasificación (prensa y noticias, pornografía,…)

- **Actualización independiente de Internet**
  Esta función permite a cualquier ordenador de la red obtener información del NOC, incluso si el ordenador no está conectado a Internet.

  La función de Actualización independiente de Internet permite usar el servicio en ordenadores no conectados a Internet. Para usar esta función, al menos una de las estaciones de trabajo de la subred (LAN) debe tener una conexión con Internet capaz de comunicarse con el NOC. Esta estación de trabajo se configura como servidor *relay*(servidor de retransmisión), y los otros ordenadores se conectan con el NOC por medio de él. El funcionamiento es el siguiente:

  - El servidor de retransmisión descarga un catálogo de actualizaciones desde el NOC cuando así se lo solicita otra estación de trabajo que no ha logrado conectar directamente con el NOC.

  - La estación de trabajo sin conexión con Internet descarga las actualizaciones necesarias desde el NOC por medio del servidor de retransmisión.

  Encontrará más información sobre la configuración de ordenadores como servidores de retransmisión en *el Capítulo 3 en “Otros métodos de instalación”.*

- **Tecnología Rumor**
  Esta función permite que todos los ordenadores de un grupo de trabajo compartan los archivos descargados, lo que evita que cada ordenador tenga que conectarse al NOC cada vez que necesite un archivo actualizado.





Rumor es un proceso por medio del cual una estación de trabajo comparte actualizaciones con otros ordenadores de la red local (LAN), lo que evita que cada ordenador tenga que actualizarse individualmente desde el NOC. Esta función reduce la carga de tráfico de Internet en la red.

La tecnología Rumor funciona como sigue:

- Cada estación de trabajo recupera del NOC información de versión sobre el catálogo más reciente. Este catálogo contiene información sobre la versión actual de cada componente de ***Antivirus*** y se almacena con una firma digital en formato de archivo .CAB
  - Si la versión es la misma que ya tiene la estación de trabajo, el proceso no continúa.
  - Si la versión es distinta de la que presente en la estación de trabajo, ésta trata de recuperar la más reciente del archivo de catálogo de sus iguales; para ello pregunta a los ordenadores de la LAN si han descargado ya la nueva actualización.

- La estación de trabajo recupera el catálogo solicitado (directamente desde el NOC o desde uno de sus iguales). Utiliza este archivo de catálogo para determinar si hay nuevos componentes.

- Si los hay, la estación de trabajo trata de recuperarlos a partir de sus iguales, preguntando a los ordenadores de la LAN si ya han descargado componentes nuevos.
  - En caso afirmativo, recupera la actualización a partir de un ordenador local (las firmas digitales vuelven a comprobarse para verificar si la estación de trabajo consultada contiene un archivo de firmas válido).
  - En caso negativo, la estación de trabajo recupera la actualización directamente desde el NOC.

Una vez recuperada la actualización, se extrae el archivo .CAB y se instalan los componentes nuevos.

# 3. Instalación de PC Seguro

## Requisitos del Sistema

El servicio se ha diseñado para sistemas operativos Microsoft Windows que se ejecutan en plataformas PC. Se instala y funciona en servidores y estaciones de trabajo con:

- **Procesador:** Intel® Pentium® o una arquitectura compatible.
- **Navegador:** Microsoft® Internet Explorer 7 o superior, Mozilla firefox 3.0 o superior, Google Chrome versión 4.0 o superior.
- **Estaciones de trabajo*:** Windows XP Home o Professional con Service Pack 2 o superior (32 bits y 64 bits), Windows Vista (32 bits y 64 bits), Windows 7 (32 bits y 64 bits) y Windows 8 (32 bits y 64 bits).
- **Servidores*:** Windows 2003 Standard Server, Windows 2003 Enterprise Server, Windows 2003 Web Edition, Windows 2003 Small Business Server, Windows 2008 (32 bits y 64 bits) Standard Server, Windows 2008 (32 bits y 64 bits) Enterprise Server, Windows 2008 (32 bits y 64 bits) Small Business Server, Microsoft Windows Server 2008 R2 Standard y Enterprise, Microsoft Windows Server 2011: Small Business Server y Microsoft Windows Server 2012





- **Requerimientos de memoria RAM*:** 1 GB mínimo (se recomienda 2GB).

* Para los productos basados en la versión 6.0 de McAfee TPS.

## Desinstalación de aplicaciones antivirus anteriores

El servicio ofrece la más reciente tecnología antivirus. Sin embargo, otras aplicaciones antivirus instaladas en el equipo pueden interferir con las avanzadas características de ***Antivirus***. Cuando varios motores de exploración antivirus tratan de acceder a los mismos archivos del ordenador, interfieren unos con otros. Si durante la instalación recibe mensajes en el sentido de que en su sistema hay otras aplicaciones antivirus, siga las instrucciones que aparecerán para desinstalarlas.
La lista siguiente recoge todos los productos que ***PC Seguro*** desinstala automáticamente.

| | |
|---|---|
| **McAfee para empresas** | · Anti-Spyware Enterprise (todas las ediciones)<br>· ePO agent<br>· Managed VirusScan y Managed Desktop Firewall (ediciones anteriores)<br>· Total Protection Enterprise<br>· VirusScan Enterprise 7.0 / 7.1 / 8.0i / 8.5i<br>· VirusScan 4.5.1 para 9x<br>· VirusScan 4.5.1 para NT, 2K, XP<br>· VirusScan 4.5.1 SP1 para 9x |
| **McAfee para usuarios particulares** | · Internet Security Suite<br>· McAfee SecurityCenter<br>· Total Protection para usuarios particulares<br>· VirusScan Retail 8.0<br>· VirusScan Professional Edition 7.0<br>· VirusScan Home Edition 7.0<br>· VirusScan Professional Edition 6.0<br>· VirusScan Home Edition 6.0<br>· VirusScan Retail 5.1.X<br>· VirusScan Retail 5.0 para 9x<br>· VirusScan Retail-OEM 4.0.3 para 9x |
| **Computer Associates** | · eTrust AntiVirus 7.1<br>· eTrust AntiVirus 7.0<br>· Inoculate IT 3.5.1<br>· Inoculate IT 4.5.3<br>· Pest Patrol para software espía |
| **Finjan** | · SurfinShield Corporate |
| **F-Secure** | · AntiVirus 5.52 Antivirus 2004 (home)<br>· Antivirus Client Security (sólo desinstalar antivirus)<br>· F-Secure Internet Security 2006 |
| **Kaspersky** | · AntiVirus Personal<br>· AntiVirus Personal Pro<br>· Antivirus Business Optimal |
| **Norton/Symantec** | · Norton Internet Security 2004 (ediciones "home" y "small ofice"): desinstala el AV<br><br>· NAV 2006 Internet Security Edition (sólo desinstala el AV)<br>· NAV 2006 (ediciones 'home' y 'small office')<br>· NAV 2006 Professional<br>· NAV 7.6 para Windows para 9x<br>· NAV 7.6 para Windows para NT<br>· NAV 7.5.1<br>· Norton Internet Security 2004 Professional (ediciones 'home' y 'small office'): desinstala el AV<br>· NAV 2004 (ediciones 'home' y 'small office')<br>· Symantec Antivirus 9.0 (small business)<br>· Norton Systemworks 2002 (sólo desinstala el AV)<br>· Symantec Systemworks 2004 (sólo desinstala el AV)<br>· Symantec Antivirus Corporate Edition 8.1<br>· NAV 2004 Internet Security Edition (sólo desinstala el AV) |

| | |
|---|---|
| | · NAV 2004 Professional<br>· NAV 2000<br>· NAV Anti-Virus Retail 2000<br>· NAV 2001<br>· NAV 2002<br>· NAV 8.0<br>· NAV 7.6 para Windows para 9X, NT<br>· NAV 7.5.1<br>· NAV 7.5<br>· NAV 7.0 Corporate Edition<br>· NAV 5.0 para Windows para 9X, NT<br>· NAV Central Quarantine<br>· NAV Quarantine Console Snap-in<br>· Norton Mobile Update Agent<br>· Norton Mobile Update Distribution Console<br>· Norton Rescue Disk |
| **Panda** | · AntiVirus 2.0<br>· Platinum Internet Security<br>· Antivirus Platinum 7.0<br>· Titanium Antivirus 2004, 2003, 2002<br>· BusinessSecure AntiVirus (ClientShield es la sección antivirus)<br>· WebAdmin Antivirus |
| **Sophos** | · Sophos Antivirus |
| **Trend Micro** | - PC-Cillin Internet Security<br>- PC-Cillin 2004<br>- OfficeScan Corporate Edition<br>- Pc-Cillin 2002<br>- OfficeScan<br>- Virusbuster 2001 for 9x and NT<br>- Virusbuster 2000 for 9x and NT<br>- Virusbuster Corporate HTTP Client NT & 2000<br>- Virusbuster Corporate HTTP Client 9x<br>- Virusbuster Corporate FILEbase Client NT & 2000<br>- Virusbuster Corporate FILEbase Client 9x<br>- Trend Micro HouseCall (On-Line) |
| | |

Si tiene algún software antivirus y/o firewall que no está en esta lista o si, por directiva del propio Windows y/o del software antivirus/firewall de terceros no se puede desinstalarlo automáticamente, debe desinstalarlos manualmente antes de instalar ***PC Seguro***.

## Configuración del Navegador

**Internet Explorer 7.0 o superior**

***Antivirus*** se ha diseñado para funcionar con la configuración de seguridad predeterminada de Internet Explorer. Esto mantiene la máxima seguridad al tiempo que permite la descarga e instalación de componentes.

Si no está seguro de la configuración, siga estos pasos para modificar la seguridad de Internet Explorer:

1. En la barra de tareas de Windows, haga clic en el botón **Inicio** y a continuación seleccione **Configuración** y **Panel de control.**
2. Haga doble clic en el icono **Opciones de Internet.**
3. Seleccione la ficha **Seguridad.**
4. Haga clic en **Nivel personalizado.**
5. Seleccione **Restablecer a Media** en el menú desplegable. Haga clic en **Restablecer.**
6. Haga clic en **Aceptar** para guardar la configuración.
7. Haga clic en **Aceptar** para salir de Opciones de Internet.





NOTA: **Aunque sea obligatorio instalar el antivirus desde una ventana de Internet Explorer, el cliente podrá utilizar otro navegador para abrir las páginas web.**

## Instalación

A continuación, guarde todo el trabajo y cierre todas las aplicaciones abiertas. Después de instalar las protecciones, debe reiniciar el ordenador.

Una vez contratado el servicio, le llegará un e-mail de Bienvenida al servicio de Seguridad con un enlace directo para que pueda instalar el producto.

Además, se puede instalar desde su portal de gestión del servicio.

Si usted tiene contratado ***PC Seguro***, para instalar diríjase a la siguiente dirección web:
https://centroseguridad.negocios.movistar.es
e introduzca el usuario y contraseña proporcionado para el servicio.

3. Identifíquese con su usuario y contraseña.
4. Seleccione la opción de gestionar el producto contratado.








Como continuación del proceso de instalación (cualquiera que sea la modalidad comercial que tenga contratada):

1. Localice el apartado **Mis Servicios** de la pestaña **Instalación** y haga clic en seleccione **Iniciar la instalación en este equipo.**

2. Si se abre algún cuadro de diálogo, haga clic en **Sí** para continuar. Si el asistente de instalación no se abre automáticamente, haga clic en **Inicio.** Si el asistente de instalación detecta otros programas Antivirus instalados en su ordenador, presentará una lista de ellos.

3. Haga clic en **Sí** (opción muy recomendable) para eliminar los productos detectados y reinicie el ordenador para continuar con la instalación. Cuando vuelva a arrancar el ordenador, aparecerá de nuevo el asistente de instalación, que le preguntará si quiere continuar con la instalación.

4. Haga clic en **Siguiente** para continuar con la instalación.

5. Si el asistente de instalación se lo pide, haga clic en **Reiniciar** para reiniciar el ordenador. Se abrirá un cuadro de diálogo de bienvenida en cuanto vuelva a arrancar Windows después de la instalación.

### Otros Métodos de Instalación

También dispone de otros métodos para instalar Antivirus y Firewall en su máquina o en otros equipos si ha ampliado licencias. Los métodos son:

- **Instalación vía URL.** En el Apartado **Mis Servicios** pulsar en el enlace **Recuperar URL de Instalación**.
- **Instalación silenciosa.** Ver apartado correspondiente en la pestaña **Instalación**.
- **Instalación remota.** Ver apartado correspondiente en la pestaña **Instalación**.





Adicionalmente en el Centro Seguridad, dispone del botón ***“¿Necesita ayuda?”*** en el que podrá acceder a toda la **documentación** disponible del servicio: manuales de usuario, guías rápidas y de administración así como obtener la información que necesite en **Soporte Técnico**.

Para más detalles sobre cada uno de los métodos pulse en el enlace que se encuentra en el recuadro Instalación.

Aparecen las siguientes pestañas:

- **Informes** con los apartados: “**Panel**”, “**Equipos**”, “**Informes**” y “**Directivas**”. Para mayor información sobre generación de informes se puede consultar el *capítulo 4 Uso.*

- **Instalación** con varios apartados: “**Mis Servicios**” donde podrá iniciar la instalación en local y recuperar la URL de instalación directa para facilitarle la misma en otros equipos. Los apartados “**Instalación Común**”, “**Instalación Silenciosa**” e “**Instalación Remota**” ofrecen distintos métodos de instalación así como utilidades que pueden ser necesarias dependiendo del método elegido.

- **Utilidades**, donde podrá disponer de las siguientes herramientas útiles: “**Escaneo Rápido (FreeScan)**” (análisis del PC para detectar si el ordenador está libre de virus), “**ContraVirus (Stinger)**” (realiza un análisis específico para una serie de virus, troyanos y variantes), “**Diagnóstico (MerTool)**” Herramienta de Escalación Mínima(herramienta necesaria para abrir una incidencia técnica, permite compilar datos de la configuración del equipo), “**CD de Arranque (CleanBoot)**” y “**Desinstalador**” (herramienta que eliminar componentes de Antivirus y/o Firewall de instalaciones anteriores que hayan quedado en el equipo).

- **Mi cuenta** donde podrá modificar sus datos que nos facilitarán comunicarle cualquier información importante que pueda ser de su interés. Además podrá configurar la periodicidad de envío del Informe de Seguridad.

# 4. Uso

**Tipos de Usuario**

El cliente puede definir distintos tipos de usuario en su red con distintos permisos. Normalmente es aconsejable definir la figura de un usuario **administrador** (para más información ver manual de administrador)**,** aquel que tiene todos los permisos para gestionar, crear y modificar las políticas de seguridad.

Por otro lado está la figura del **usuario** del equipo cuyos permisos son asignados por el usuario **administrador**. Como opciones, puede darle permiso total o por el contrario hacer que este usuario no tenga decisión alguna sobre acciones a realizar.

- **Administrador.** Aquel que tiene todos los permisos y asigna los correspondientes al resto.
- **Usuario del equipo.** Aquel cuyos permisos han sido designados por el administrador.

**Exploración**

**Funcionamiento de *Antivirus***

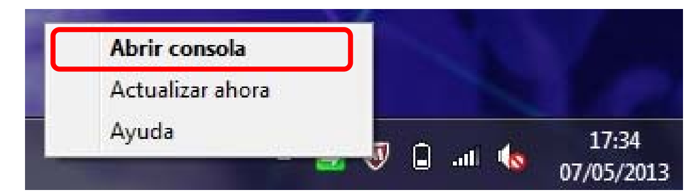
La configuración predeterminada de ***Antivirus*** es explorar todos los archivos y carpetas del ordenador cada vez que se acceda a ellos. Los mensajes de correo electrónico no se exploran

cuando se reciben, sino en el momento de abrirlos. El responsable de la configuración del analizador en tiempo real es el propio fabricante del producto de ***Antivirus***.

### Análisis del equipo

La función **Analizar equipo** permite explorar una unidad o carpeta determinadas en cualquier momento. Para especificar una exploración:

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows.
2. Seleccione **Abrir Consola**.




3. En la ventana de la consola, ir a **Menú Acción** y seleccione **Analizar equipo**.




4. Especifique si desea explorar todo el equipo o analizar una unidad o carpeta específica. Una vez seleccionada la ubicación del análisis, hacer clic en **Iniciar Análisis**.
5. Una vez terminada el análisis, podrá cerrar la ventana o hacer clic en el botón **Ver informe detallado** para obtener más información.

Después de ejecutar el análisis en una carpeta o unidad, puede hacer clic en el botón **Ver informe detallado** para ver el informe de la exploración. El informe de la exploración presentará los siguientes datos: fecha/hora de inicio de la exploración, tiempo de exploración, nivel de actualización de *Antivirus,* fecha de la última actualización, elementos explorados y número de infecciones





detectadas, lista de archivos infectados si los hubiera inclusive previo a la instalación del producto en el PC.

Para la lista de archivos la situación puede ser una de las siguientes:

- **Limpio:** el archivo se ha limpiado de la infección.
- **En Cuarentena:** el archivo no se ha podido limpiar; por tanto, se ha guardado en la cuarentena.

## 5. Configuración de Firewall

### Configuración inicial de Firewall

Haga clic en el botón secundario del icono de la Protección ( ) situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola.**
A continuación definimos las principales características que puede definir un usuario en el módulo Firewall.

En la ventana/consola:

- En **Protección con firewall:** comprobar si está *Activada* o *Desactivada* (estado de *Módulo Firewall*). En **Menú** Acción, opción **Detalles del producto**¸ podrá cambiar el estado de firewall a Activado o Desactivado.
- En **Menú Acción**, opción **Establecer tipo de conexión:**
  - **Red no fiable** (el equipo no puede comunicarse con otros equipos de la red local o de Internet). Seleccione esta conexión si está conectado directamente a Internet en, por ejemplo: a través de una conexión de marcación, una línea ADSL o un cable módem; mediante un tipo de conexión en un cibercafé, hotel o aeropuerto.
  - **Red de confianza** (el equipo puede comunicarse con otros equipos de la red local. Determinados servicios, especificados por el administrador, pueden tener acceso a Internet). Seleccione este tipo de conexión si está conectado indirectamente en una red separada de Internet por un cortafuegos o enrutador de hardware. Por ejemplo: en una red doméstica o en la de la oficina.
  - **Personalizada** (el equipo sólo puede comunicarse con aquellas direcciones IP y servicios especificados por el administrador). Seleccione esta opción si sólo debe permitir las comunicaciones desde servicios del sistema a través de puertos específicos o desde un rango específico de direcciones IP, o bien si se trata de un servidor que proporciona servicios del sistema.

  Seleccione su caso y al cerrar la ventana, confirme que desea guarda la configuración del firewall.

En **Menú Acción**, opción **Ver lista de aplicaciones**:
Lista de aplicaciones que intentar acceder a Internet desde su ordenador. Inicialmente existen una serie de aplicaciones que por defecto están permitidas:

- MYAGTSVC (Agente de la protección)
- UPDDLG (Actualizar módulos de la protección)
- IEXPLORE (Internet Explorer)
- SVCHOST (SO Windows)
- SERVICES (SO Windows)
- LSASS (SO Windows)
- USERINIT (SO Windows)

- o WINLOGON (SO Windows)
- o EXPLORER (SO Windows)

Una vez seleccionada la casilla de una aplicación, se podrá **Aprobar** o **Bloquear** haciendo clic sobre los botones para tal fin. Inicialmente cualquier otra aplicación que trate de establecer una conexión a la red mientras están desactivadas las notificaciones será bloqueada.

## Configuración de una conexión personalizada

Haga clic con el botón derecho del ratón sobre el icono de la Protección , haga clic en **Abrir consola.** Una vez abierta la ventana de la consola, ir a **Menú Acción**, y hacer clic en la opción **Establecer tipo de conexión.** Si modifica el tipo de conexión de firewall a *Personalizada*, puede personalizarlo haciendo clic sobre el botón **Editar**. El proceso de personalización permite designar lo siguiente:

- Los equipos que pueden conectarse al suyo. Se puede configurar un intervalo de IP específico a través de las que el equipo puede recibir las comunicaciones, lo que permite limitar las comunicaciones a determinadas direcciones IP.

- Puertos a través de los que el equipo puede recibir las comunicaciones, necesario para configurar el equipo como un servidor que proporciona servicios del sistema. El equipo aceptará las comunicaciones a través de un puerto abierto del equipo.

En el cuadro de diálogo que figura en esta ventana, puede definir con exactitud las comunicaciones que el servicio de protección de firewall permite:

Determinadas aplicaciones, entre las que se encuentran servidores web y programas de servidor que comparten archivos, deben aceptar conexiones no solicitadas de otros equipos a través de los puertos designados de servicios del sistema. Al configurar un modo de funcionamiento personalizado, puede llevar a cabo lo siguiente:

- o Permitir que las aplicaciones actúen como servidores en una red local o en Internet.
- o Agregar servicio aprobado.
- o Quitar o eliminar un servicio de la lista.

Seleccione un puerto de los servicios del sistema sólo sí está seguro de que debe abrirse. No es muy habitual que necesite abrir un puerto. Se recomienda desactivar los servicios del sistema sin uso para evitar intrusiones.

A continuación se presentan ejemplos de servicios del sistema que generalmente necesitan que los puertos se abran:

- o Servidor de correo electrónico: no es necesario abrir el puerto del servidor de correo para recibir los mensajes de correo electrónico. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de firewall actúa como un servidor de correo.
- o Servidor web: no es necesario abrir un puerto del servidor web para ejecutar un navegador web. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de Firewall actúa como un navegador web.

- **Puertos del servicio del sistema estándar**





Los servicios del sistema se comunican con Internet a través de los *puertos*, que constituyen conexiones lógicas. Los servicios habituales del sistema de Windows se relacionan generalmente con *puertos de servicio* particulares, y el sistema operativo del equipo u otras aplicaciones del sistema pueden intentar abrirlos. Teniendo en cuenta que estos puertos pueden suponer una fuente de intrusiones para el sistema, debe abrirlos en la configuración predeterminada antes de que equipos externos puedan acceder a ellos.

Estos puertos de servicio estándar utilizados habitualmente se enumeran de manera predeterminada en el cuadro de diálogo **Configuración personalizada**, donde puede abrirlos y cerrarlos:

- Puertos 20-21 del protocolo de transferencia de archivos (FTP, File Transfer Protocol);
- Puerto 143 del servidor de correo (IMAP);
- Puerto 110 del servidor de correo (POP);
- Puerto 25 del servidor de correo (SMTP);
- Puerto 445 de Microsoft Directory Server (MSFT DS);
- Puerto 1433 de Microsoft SQL Server (MSFT SQL);
- Puerto 3389 de Remote Assistance/Terminal Server (RDP);
- Puerto 135 de llamadas de procedimiento remoto (RPC, Remote Procedure Calls);
- Puerto 443 del servidor web seguro (HTTPS);
- Puerto 5000 de Plug and Play universal (UPNP);
- Puerto 80 del servidor web (HTTPS);
- Puertos 137 a 139 de Windows File Sharing / Ficheros y carpetas compartidas (NETBIOS).

Los puertos que no aparecen en la lista del cuadro de diálogo **Configuración personalizada del cortafuegos** no están supervisados por el servicio de protección de firewall. Se permitirán las comunicaciones a través de los puertos que no aparecen en la lista. Para bloquear un puerto, debe añadirlo a esta lista y asegurarse de que se ha cancelado su selección.

**Apertura de un puerto de servicio.**

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola**.
2. En la ventana de la consola, ir a **Menú Acción** y haga clic en **Establecer tipo de conexión**.
3. Haga clic en **Personalizada**, a continuación, haga clic en el botón **Editar**.
4. En el cuadro de diálogo **Configuración personalizada del firewall**, seleccione las casillas de verificación situadas junto a los puertos de servicio que desea abrir. El equipo aceptará todas las comunicaciones que se produzcan a través de estos puertos.

Seleccione un puerto en la lista de ***conexiones desde los siguientes servicios*** sólo si está seguro de que se debe abrir. Se recomienda desactivar los servicios del sistema sin uso para evitar las intrusiones.

5. Al cerrar la consola, deberá confirmar que desea guarda la configuración del cortafuegos.

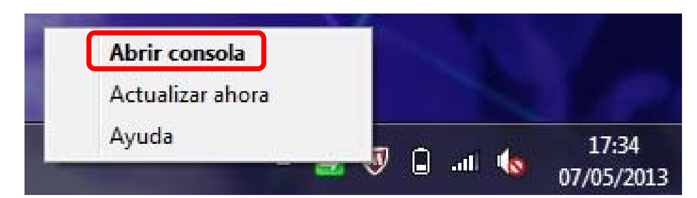
- **Adición y Edición de puertos en servicio**

**Ejemplo:**
**Permitir el uso compartido de archivos e impresoras**

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola**.








2. En la ventana de la consola, ir a **Menú Acción** y haga clic en **Establecer tipo de conexión**.
3. Haga clic en **Personalizada**, a continuación, haga clic en el botón **Editar**.
4. Haga clic en **Agregar servicio aprobado.**
5. Si el servicio aparece en la lista de los servicios conocidos, p.ej. Windows File Sharing (NETBIOS) Ports 137-139, podrá seleccionarlo y hacer clic sobre el botón **Agregar.** En caso contrario, deberá especificar un servicio que no figura en el listado. Para ello, deberá especificar:
    - o Un nombre descriptivo del servicio.
    - o Un puerto o rango de puertos.
    - o Seleccione el protocolo (“idioma”) que el servicio utiliza para establecer la comunicación. Consulte la documentación de la aplicación si no está seguro del protocolo que debe seleccionar:
        - **TCP**: el protocolo de control de transmisión/protocolo de Internet es el protocolo de Internet más común y se puede utilizar como protocolo de red.
        - **UDP**: el protocolo de datagramas de usuario es menos sólido que el TCP/IP. Se utiliza habitualmente para intercambiar pequeñas unidades de datos entre el equipo de una red que utiliza el protocolo de Internet.
        - **Ambos**: TCP y UDP. Haga clic en **Aceptar**.







Nota: si la documentación de la aplicación no especifica el protocolo, se recomienda la selección de TCP/IP, ya que se trata del protocolo más utilizado. No seleccione Ambos si no se precisan los dos protocolos, ya que, de esta manera, la red será más vulnerable a las intrusiones.

6. Haga clic en **Aceptar**.

- **Para cerrar un puerto de servicio.**

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola**.
2. En la ventana de la consola, ir a **Menú Acción** y haga clic en **Establecer tipo de conexión**.
3. Ir a tipo de conexión **Personalizada**, a continuación, haga clic en el botón **Editar**.
4. En el listado de conexiones permitidas, seleccionar el servicio que desea deshabilitar/cerrar puerto de servicio.
5. Hacer clic sobre el botón **Quitar el servicio de la lista.**
6. Al cerrar la consola, deberá confirmar que desea guarda la configuración del cortafuegos.

- **Configuración de una dirección IP para una configuración personalizada.**

Además de aceptar las comunicaciones a través de los puertos de servicio seleccionados, el equipo aceptará las comunicaciones que se originen desde las direcciones IP designadas.

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola**.
2. En la ventana de la consola, ir a **Menú Acción** y haga clic en **Establecer tipo de conexión**.
3. Ir a tipo de conexión **Personalizada**, a continuación, haga clic en el botón **Editar**.
4. En el apartado de los equipos que pueden conectarse al suyo, seleccionar una de las 3 opciones:
   - Cualquier equipo.
   - Mi subred (segmento de área local).
   - Intervalo IP específico. Al seleccionar esta opción, deberá rellenar las casillas de las direcciones IP inicial y final del intervalo/rango.
5. Al cerrar la consola, deberá confirmar que desea guarda la configuración del cortafuegos.

- **Gestión de Aplicaciones de Internet.**

El Módulo Firewall supervisa las comunicaciones con las aplicaciones de Internet, que se conectan con Internet y su equipo. Cuando la protección de cortafuegos detecta una aplicación de Internet que se ejecuta en el equipo, permite que la aplicación se conecte a Internet o bloquea la conexión, en función de la configuración.

El administrador puede configurar el servicio de protección de firewall para permitir o bloquear determinadas aplicaciones de Internet, además de solicitarle una respuesta siempre que se detecte una aplicación de Internet.

**¿Cómo responde Firewall a una detección?**

Cuando la protección de cortafuegos detecta una aplicación de Internet:

1. Comprueba la lista de aplicaciones que se han detectado en el equipo.
2. Comprueba la lista de aplicaciones que se han aprobado.
3. Comprueba la "lista blanca" que se mantiene en la base de datos de McAfee.





4. Si la directiva lo permite, le solicita una respuesta; de lo contrario, bloquea la aplicación

- **¿Cómo puedo gestionar las aplicaciones de Internet detectadas?**

El servicio de protección de cortafuegos mantiene una lista de las aplicaciones de Internet que se han detectado en el equipo y que ha aprobado. Si la directiva así lo permite, podrá ver estas aplicaciones y sus permisos asignados. También puede editar los permisos o eliminar las aplicaciones de la lista.

***PARA GESTIONAR LAS APLICACIONES DE INTERNET***

1. Haga clic con el botón secundario en el icono de la Protección situado en la barra de tareas de Windows y, a continuación, seleccione **Abrir consola**.
2. En la ventana de la consola, ir a **Menú Acción** y haga clic en **Ver lista de aplicaciones**.
3. En el listado de las aplicaciones detectadas, podrá seleccionar una o varias aplicaciones. A continuación, haga clic sobre uno de los siguientes botones: **Aprobar, Bloquear** o **Suprimir.** Además se puede agregar una aplicación que todavía no figure en el listado de aplicaciones detectadas.

Al cerrar la consola, deberá confirmar que desea guarda la configuración del cortafuegos.





# 6. Centro Seguridad

## Acceso al Centro Seguridad

Si usted tiene contratado ***PC Seguro***, para acceder al Centro Seguridad, diríjase a la siguiente dirección web:

https://centroseguridad.negocios.movistar.es

e introduzca el usuario y contraseña proporcionado para el servicio.

Si usted es usuario de Pack Seguridad Total, siga los siguientes pasos:

1. Diríjase a http://www.movistar.es/packseguridadtotal
2. Acceda al apartado Gestione Online su Pack Seguridad
3. Identifíquese con el usuario y contraseña de movistar.es.
4. Seleccione la opción de Antivirus del menú y pulse: Acceda a la gestión de Antivirus

## Informes de Seguridad

**¿Cómo accedo a los informes?**
El acceso a informes se realiza desde el apartado **"Informes"** del portal Centro Seguridad.




**¿Qué tipo de información se puede obtener?**
Los Informes presentan 4 opciones: **Panel**, **Equipos**, **Informes** y **Directivas**.








**Panel** desglosa información resumida sobre el estado de los equipos y licencias instaladas. En los apartados Cobertura indica las licencias instaladas y No instaladas así como los equipos actualizados para cada módulo de la protección.

En el apartado **Equipos** se permite:
1. Encontrar algún equipo en concreto (introducir en "**Buscar equipos**" el equipo a buscar y aparecerá la información disponible).
2. Permite buscar equipos por:

- ✓ **Grupos**. Un grupo es un conjunto de equipos al que el usuario puede aplicar la misma política de seguridad. Facilitaría cualquier acción para el usuario pues si tiene 20 equipos y quiere aplicar a todos los mismos criterios, si no tuviese el grupo tendría que aplicar la directiva equipo a equipo.
- ✓ Por **Informes de actividad** de equipos por períodos: última semana y por mes.
- ✓ Por **estado** del equipo: no actualizados, aquellos que hayan tenido alguna detección en concreto, equipos bloqueados.




3. Seleccionando equipos en la casilla de verificación correspondiente se puede:
Enviar un **correo electrónico** al usuario del equipo (pulsando la opción "correo electrónico") teniendo en cuenta que enviará un e-mail a la dirección que el usuario haya introducido.





- ✓ **Eliminar** el equipo. Si el equipo ya no existe en la empresa o si se desinstalar le protección en el equipo. Al eliminarlo, se libera esta licencia para que pueda reinstalarla en el equipo o instalarla en otro.
- ✓ **Bloquear equipo**. Si, por ejemplo, no desea que realice actualización de las firmas de antivirus o no desea protegerlo.
- ✓ Incluir el equipo en algún **grupo**.

Pulsando sobre el enlace correspondiente a cada equipo aparece la información disponible de dicho equipo:

**Detalles del equipo**:

- ✓ **Nombre del Sistema**. Nombre del equipo.
- ✓ **Dirección de correo electrónico**. La indicada en la instalación (modificable)
- ✓ **Grupo al que pertenece**. Si no se indica ninguno pertenece el grupo establecido por defecto (modificable).
- ✓ **Elementos de acción**. Al pulsar el enlace nos muestra información sobre el estado del equipo. **Última conexión** con la plataforma (última conexión para descarga de firmas de antivirus – actualizaciones), **Fecha del archivo DAT** de firmas (última versión de firmas – actualización – descargada), **Versión del motor** (indica la versión del componente principal de antivirus). Además, si no se encuentra actualizado, indica una serie de pasos para identificar el problema de las actualizaciones y solucionarlo.
- ✓ **Propiedades del equipo**. Datos relevantes como: Estado del Sistema (actualizado o no), última conexión del servidor, versión archivo DAT, versión del explorador o dirección IP.
- ✓ **Detecciones.** Informa (por períodos establecidos) de las detecciones así como de las aplicaciones aprobadas (permitidas) por el usuario.

Si se produce algún cambio (modificación de grupo, correo electrónico, etc...) deberá pulsar el botón guardar para aceptar los cambios.

Propiedades del equipo

| | | | |
|---|---|---|---|
| Estado del sistema: | Actualizado | | |
| Última conexión del servidor: | 07/05/2013 | | |
| Fecha de instalación del producto: | 06/05/2013 | | |
| Versión de archivos DAT: | 7067 | Última versión de archivos DAT: | 7069.0000 |
| Fecha de los archivos DAT: | 06/05/2013 | Fecha de últimos archivos DAT: | 08/05/2013 PST |
| Idioma del producto: | ESP | | |
| Versión del motor: | 5400.1158 | | |
| Servidor de retransmisión: | No | | |
| Versión del agente: | 5.2.3 Patch 5 | | |
| Número de compilación de analizador: | 5.2.3.150 | | |
| Versión del SO: | Windows 7 Professional, 64-bit, Build 7601,Service Pack 1 | | |
| Versión del navegador: | 9.0.8112.16421 | | |
| Dirección IP: | 127.0.0.1 | | |
| Estado del último análisis planificado: | | | |
| Hora de ejecución del último análisis planificado: | | | |
| Estado de la última actualización: | Completado correctamente | | |
| Hora de la última actualización: | 07/05/2013 9:53:57 | | |
| Estado del análisis en tiempo real: | Activado | | |

**Informes detallados**

Esta opción permite al usuario ver informes de:




**Detecciones.** Muestra los resultados de todos los equipos, por grupos. Además, se puede filtrar por períodos de análisis, por tipo de detección y agrupar por equipo o detección. Muestra además los archivos detectados, la fecha de la última detección, grupo al que pertenece, etc...

**Perfiles de equipo.** Muestra y organiza los equipos por sistema operativo y/o versión del navegador Microsoft Internet Explorer.

**Equipos duplicados.** Permite optimizar y actualizar la lista de equipos que por algún motivo hayan sido dados de baja, estén obsoletos o estuvo protegidos y aquellos que lo están.

**Programas no reconocidos.** Aplicaciones no reconocidas o certificadas por McAfee que pueden ser bloqueadas por el cortafuegos o potencialmente no deseados. Permite agruparlos por programas o por equipos.

**Eventos entrantes bloqueados por cortafuegos.** La información es mostrada por períodos (última semana, mes, 3 meses y año) y se puede agrupar por equipos destino y equipos origen.

**Historial de detecciones.** Muestra gráficos por mes y trimestre tanto de las detecciones encontradas como de los equipos con detecciones.

**Otras operaciones que pueden llevarse a cabo desde el Centro Seguridad**
Las más importantes son las siguientes:

- Bloqueo/Desbloqueo de máquinas: Se consigue que la máquina bloqueada no se actualice. Se marcará en la casilla correspondiente para bloquearla o desbloquearla.
- Eliminar equipos: Se debe llevar a cabo sobre aquella máquina sobre la que se haya desinstalado el producto.

Esta es la expresión técnica de lo que sería una reasignación de licencias por parte del Administrador, es decir, si el Administrador quiere reasignar las licencias adquiridas a PC´s distintos, sólo tendrá que desinstalar el producto de Antivirus de una de las máquinas, e instalarlo en la máquina nueva. En la siguiente comunicación la máquina aparecerá con la licencia asignada en el nuevo PC. Además, las actualizaciones de ficheros de virus se realizarán a partir de ese momento sobre la nueva máquina.

- Creación/Eliminación de un grupo: Los grupos permiten organizar la información para facilitar el uso del Administrador y realizar informes por grupos. Las máquinas podrán ser





movidas de un grupo a otro para facilitar la administración. La eliminación del grupo debe ser posible sólo después de haber borrado todos los PC´s asociados.

## Directivas

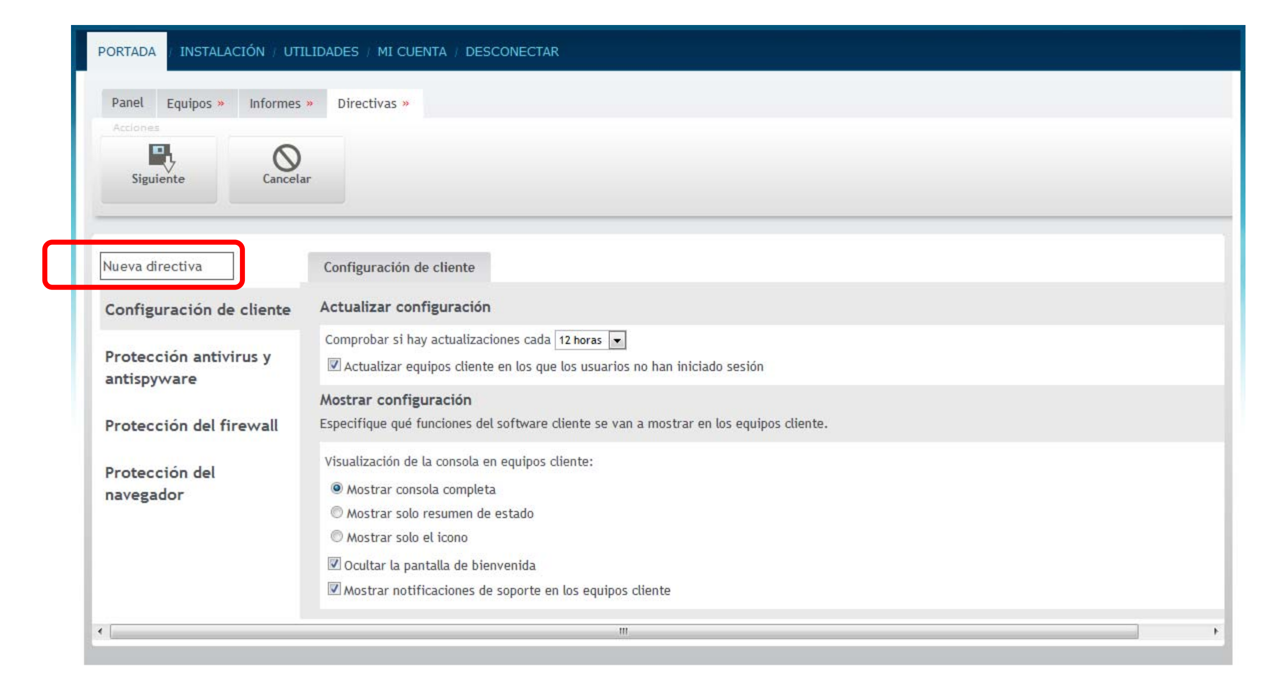
Las directivas definen la configuración de los servicios contratados, por ejemplo, si está habilitado la detección de desbordamiento de búfer, si el usuario puede configurar Firewall para permitir la salida de aplicaciones a Internet, etc. Inicialmente solo existe una única política predeterminada: McAfee Default. Al acceder al menú directiva, podemos hacer clic en **Ver directiva** McAfee Default.

Una vez que la directiva McAfee Default no se puede modificar, se puede hacer clic en **Agregar Directiva** para crear y personalizar una nueva.




## Directivas personalizadas

Al agregar una directiva personalizada, deberá elegir un nombre que identifique la directiva.

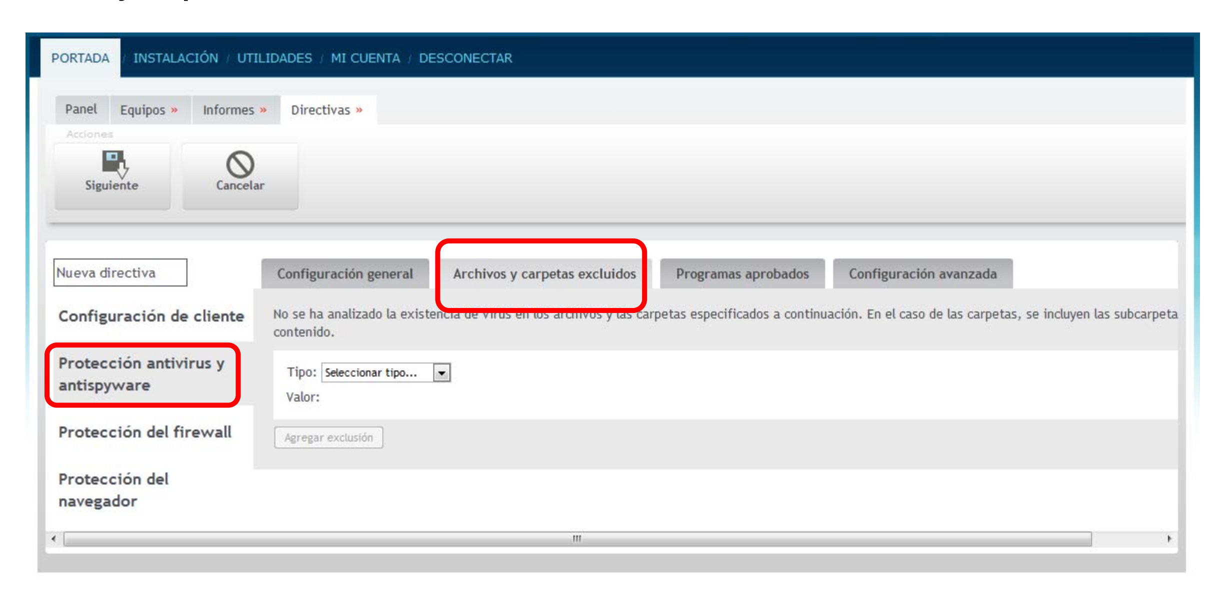







A continuación, algunos de los apartados disponibles de la configuración de la directiva.

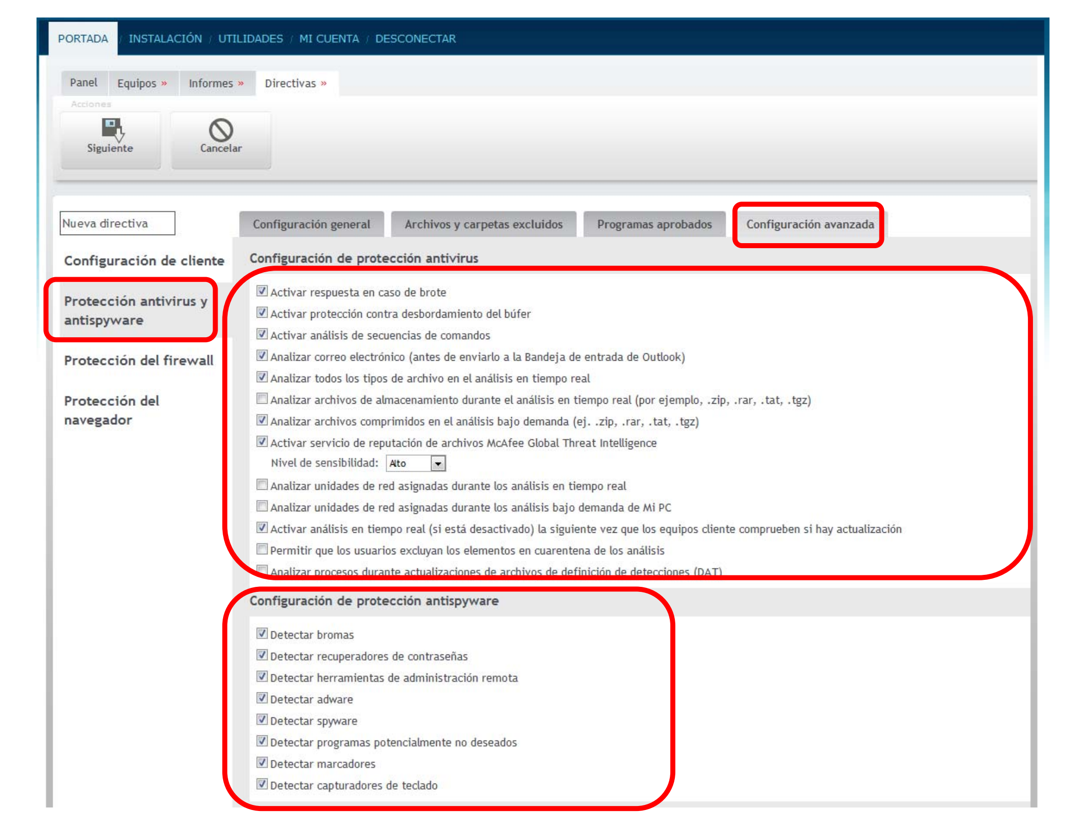
### Archivos y carpetas excluidos del análisis de Antivirus




### Configuración avanzada de Antivirus

Ejemplos de parámetros:

- Detección de desbordamiento de búfer
- Verificación de la red heurística Artemis (detección de archivos sospechosos)
- Detección de herramientas de administración remota







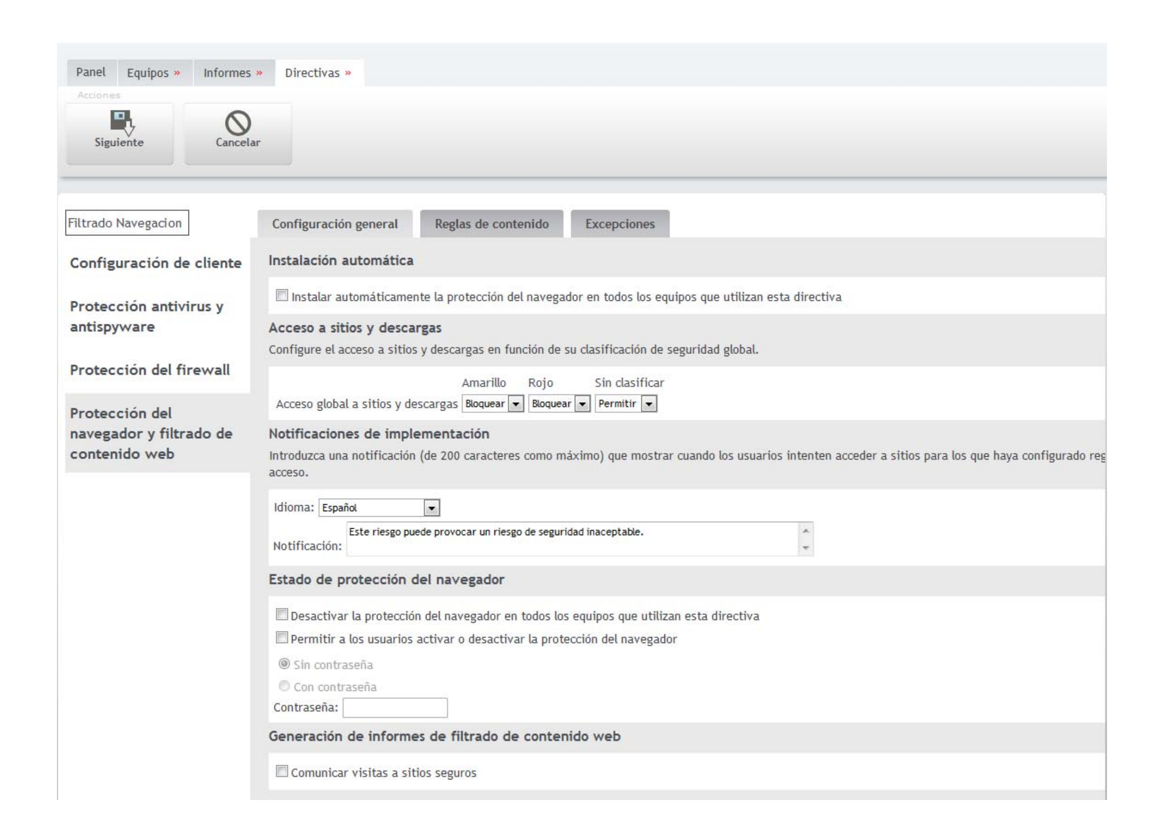

Una vez configurada la directiva, haga clic en el botón **Siguiente**. A continuación, podrá asignar la directiva a un grupo de equipos o equipos seleccionados de una lista. Una vez aplicada, haga clic sobre el botón **Guardar**.

**Configuración de filtrado de contenido Web**

A través de este menú el usuario puede configurar diferentes opciones para proteger la navegación en Internet y el acceso a sitios web.

La configuración de estos parámetros se realiza accediendo a la opción **Protección del navegador y filtrado de contenido web** dentro de las opciones de creación de las Directivas:

- Instalación automática: permite seleccionar si la opción de protección de navegación se instalará automáticamente en los equipos que empleen esta directiva
- Acceso a sitios y descargas: McAfee clasifica los sitios web en función de su reputación, que refleja su nivel de peligrosidad y riesgo al acceder a ellos. Dicha clasificación se basa en tres niveles: Rojo, Amarillo y verde en función de su peligrosidad. En esta opción de menú cómo se comportará el producto cuando se acceda a sitios web que estén clasificados en alguna de estas categorías.
- Notificaciones de implementación: cuando se acceda a un sitio web considerado como peligroso el usuario recibirá un mensaje de notificación. El contenido de dicha notificación puede ser cambiado en esta opción de menú.
- Estado de protección del navegado: permite que el usuario pueda activar o desactivar la protección en su equipo.




Las **Reglas de contenido** permiten controlar el acceso a sitios web por parte de los usuarios. Se pueden definir reglas de control de acceso a determinados sitios web o a categorías de sitios web. El control del acceso se hace en base a categorías de contenidos que pueden ser seleccionadas de la lista. Estas categorías están clasificadas en base a diferentes Grupos funcionales.

Panel | Equipos » | Informes » | Directivas »

Acciones

Siguiente | Cancelar

Filtrado Navegacion

Configuración de cliente

Protección antivirus y antispyware

Protección del firewall

Protección del navegador y filtrado de contenido web

Configuración general | Reglas de contenido | Excepciones

La protección del navegador permite controlar el acceso de los usuarios a los sitios en función de su contenido. Utilice esta lista para especificar los tipos contenido cuyo acceso es permitido o bloqueado por la protección del navegador o para los que se muestra una advertencia. **Tenga presente que ahora s bloquean de manera predeterminada ciertas categorías relacionadas con la seguridad** (por ejemplo, phishing, malware y spam); puede cambiar este comportamiento creando o editando una directiva personalizada.

Filtros

Utilice las opciones situadas en la parte superior de la lista para filtrar y ordenar la lista de contenido. A continuación, seleccione las categorías de con y haga clic en **Permitir**, **Advertir** o **Bloquear**.

Grupo funcional: Todos

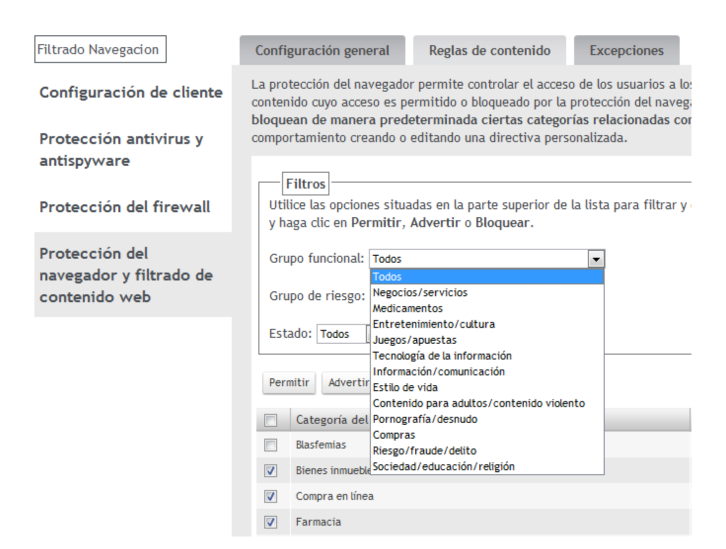
Grupo de riesgo: Todos

Estado: Todos

Permitir | Advertir | Bloquear

| | Categoría del contenido | Grupo funcional | Grupo de riesgo | Esta |
|---|---|---|---|---|
| ☐ | Blasfemias | Contenido para adultos/contenido violento | Propiedad | Ad |
| ☑ | Bienes inmuebles | Compras | Productividad | Per |
| ☑ | Compra en línea | Compras | Productividad | Per |
| ☑ | Farmacia | Compras | Productividad | Per |
| ☐ | Marketing/comercio | Compras | Productividad | Per |
| ☐ | Moda/belleza | Compras | Productividad | Per |
| ☐ | Subastas/clasificados | Compras | Productividad | Per |
| ☐ | Vehículos a motor | Compras | Productividad | Per |
| ☐ | Armas | Contenido para adultos/contenido violento | Propiedad | Per |
| ☐ | Contenido desagradable | Contenido para adultos/contenido violento | Propiedad | Per |
| ☐ | Extremo | Contenido para adultos/contenido violento | Propiedad | Pe |
| ☐ | Violencia | Contenido para adultos/contenido violento | Propiedad | Perm |

Hay una lista de 12 grupos funcionales en los que están clasificadas las URLs:



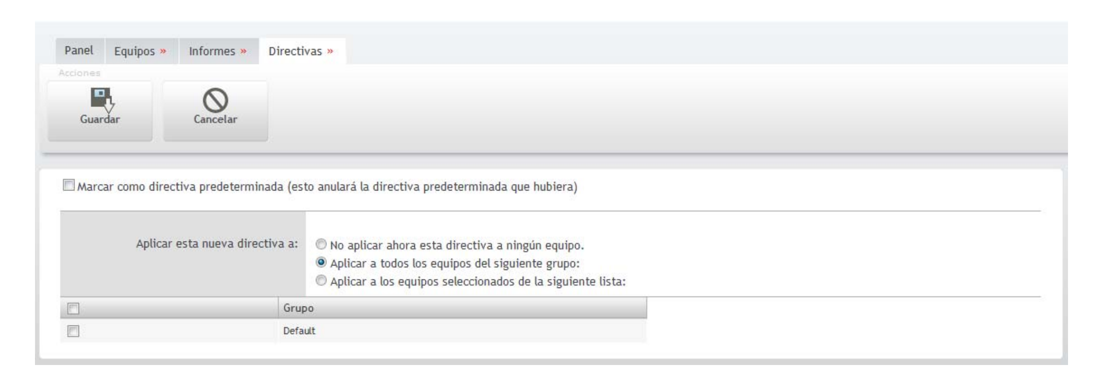

En caso necesario, se pueden crear listas de excepciones que contengan URLs específicas que se deseen permitir o bloquear. Por ejemplo, puede que se desee limitar el acceso a prensa y periódicos pero que se desee permitir el acceso a una web en particular.








Por último, una vez creada la Directiva se puede seleccionar si se desea aplicar a todos los equipos de un grupo en particular o bien seleccionar manualmente los equipos de una lista




# 7. Utilidades

**¿En qué consisten? ¿Cómo funcionan?**

Son 4 herramientas contrastadas y útiles en materia de detección y eliminación de virus. Se incorpora además la utilidad *Desinstalación.* Las herramientas están disponibles en el Centro Seguridad. A continuación, el listado de las herramientas:

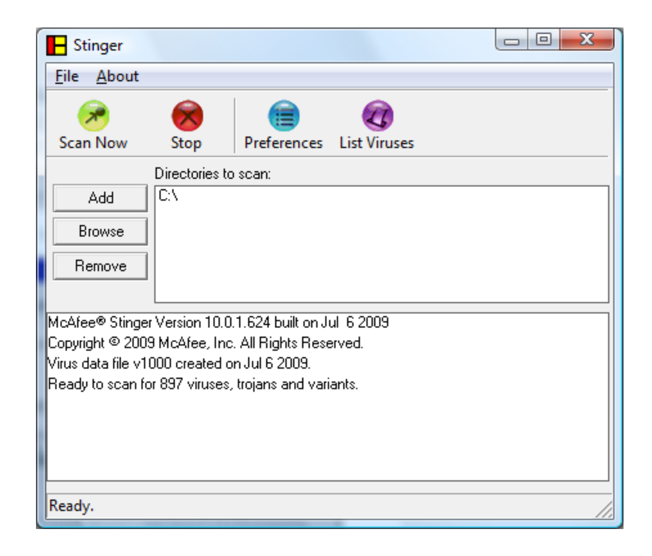
1. **Escaneo Rápico (FreeScan)**. Herramienta gratuita que permite detectar virus en un PC. Inicia un escaneo de manera que al realizarlo emite un informe. Es una herramienta útil cuando por ejemplo se desea incorporar algún elemento a la red . Se accede (ver figura)

Al solicitar ***escanear ahora*** se inicia el proceso, preguntándonos antes la herramienta qué unidades, carpetas o documentos deseamos escanear de manera que en unos minutos está disponible el informe.

2. **ContraVirus (Stinger).** Esta utilidad consiste en un análisis más avanzado que el realizado por *FreeScan* en el aspecto que incluye troyanos y modificaciones que hayan podido tener éstos y los virus. El proceso es sencillo y tras la descarga o su ejecución en Internet simplemente hay que pulsar ***Scan Now***, realizando antes la selección de las unidades o carpetas que deseamos analizar. Esto se realiza mediante el botón ***Browse***. En la figura se puede observar:



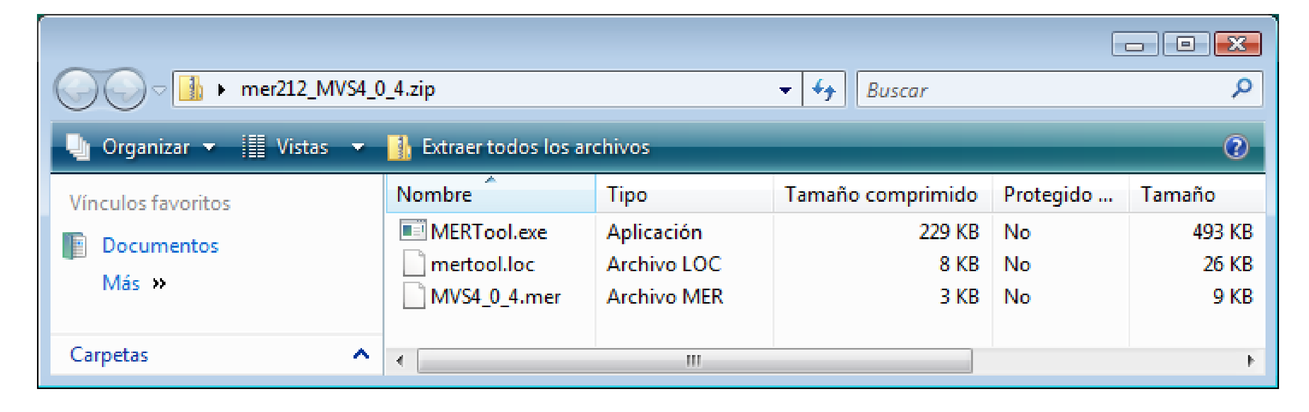





3. **Diagnóstico (MER Tool)** o Herramienta de Escalación Mínima. Se trata de una opción del proveedor de software que permite compilar datos de la configuración del equipo.
Para usarlo hay que hacer clic en el enlace que nos solicitará que la aplicación pueda ser descargada en el PC o ejecutada desde Internet.
Se trata de 3 archivos donde aconsejamos abrir primero el archivo leeme.txt que incluye las instrucciones del proceso, entre ellas rellenar la hoja Excel donde hay que responder una serie de cuestiones sobre el PC, el sistema y también relativas a la Red de Área Local, equipamiento, etc… así como describir el problema.

Siguiendo las instrucciones del archivo de texto (5 pasos) llegamos a la última en la que se indica envíe por correo electrónico la información solicitada y puesta en formato .ZIP para ocupar el mínimo espacio posible.

A continuación mostramos la imagen de los 3 archivos iniciales (entre ellos el archivo de texto).




4. **CD de Arranque (Clean Boot).** Con esta herramienta puede crear un CD, siguiendo las instrucciones dadas en la pantalla, que le permitirá, en caso de tener su equipo infectado por un virus, arrancar el pc desde la unidad CD-ROM y ejecutar ***Antivirus***, lo que le facilitará eliminar o desinfectar aquellos archivos dañados. Conviene tener en cuenta que el CD es actualizado constantemente con las firmas correspondientes a los últimos virus.

5. **Desinstalador**. Esta utilidad permite buscar y eliminar componentes de Antivirus y/o Firewall PC de instalaciones anteriores que hayan quedado en el equipo garantizando una reinstalación de Antivirus y/o Firewall PC desde cero.



